ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය | நிதியியல் உளவறிதற் பிரிவு | Financial Intelligence Unit

Guidelines -- 03/2018

18 April 2018

Ref: 037/08/001/0006/018

To: CEO / General Manager/ Proprietor

Dear Sir / Madam,

Guidelines on Anti-Money Laundering/Countering the Financing of Terrorism Compliance Obligations for Dealers in Real Estate, Precious Metals, Precious and Semi-Precious Stones, No. 03 of 2018

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Designated Non-Finance Business (Customer Due Diligence) Rules No. 1 of 2018.

Yours faithfully

D M Rupasinghe
Director
Financial Intelligence Unit

Cc : Compliance Officer

14 වන මහල, අංක 30, ජනාධිපති මාවත,
තැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව

14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை
த. பெ. இல. 590, கொழும்பு 01, இலங்கை

Level 14, No. 30, Janadhipathi Mawatha,
P. O. Box. 590, Colombo 01, Sri Lanka.

94 11 2477125 / 509 | 94 11 2477692 | fiu@cbsl.lk | www.fiusrilanka.gov.lk

Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism Compliance Obligations for Dealers in Real Estate and Precious Metals, Precious and Semi-Precious Stones, No 03 of 2018

PART I
Introduction

1. The Financial Intelligence Unit (FIU) acting within the powers vested with it under the Financial Transactions Reporting Act, No. 6 of 2006 (hereinafter referred to as "FTRA"), issued the Designated Non-Finance Business (Customer Due Diligence) Rules No. 1 of 2018 (hereinafter referred to as "CDD Rules") by Gazette Extraordinary No. 2053/20 dated 2018.01.10 which is applicable to institutions carrying out non-financial businesses and professions.

2. As described in the CDD Rules, these Guidelines shall apply to following Designated Non-Finance Businesses (DNFBs, hereinafter referred to as "Institution(s)").

   - **Real estate agents**, when they are involved in transactions for their customers in relation to the buying and selling of real estate
   - **Dealers in precious metals and dealers in precious and semi-precious stones**, including but not limited to, metals and stones covered by the National Gem and Jewellery Authority Act, No. 50 of 1993

3. These Guidelines are issued for the purpose of identifying, assessing and managing Money Laundering (ML) and Terrorist Financing (TF) risks.

4. For the purpose of this Guideline, unless the context otherwise requires:
   - **AML/CFT** means Anti-Money Laundering and/or the Countering the Financing of Terrorism as recommended by the Financial Action Task Force
   - **CDD** means Customer Due Diligence;

- **FATF** means the Financial Action Task Force (The global policy setter against Money Laundering and Financing of Terrorism);
- **FIU** means the Financial Intelligence Unit which is designated for the purposes of the Financial Transactions Reporting Act, No. 6 of 2006 [Gazette (Extraordinary) No: 1437/24 dated 23.03.2006], and charged with the implementation and administration of the provisions of the said Act;
- **ML** means the offence of money laundering, as defined in and punishable under Section 3 of the Prevention of Money Laundering Act, No 5 of 2006
- **ML/TF** means Money Laundering/Terrorist Financing
- **PEPs** mean Politically Exposed Persons, including individuals in Sri Lanka or abroad who are, or have been, entrusted with prominent public functions. For example: heads of state or of government, a politician, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. The family members and close associates of PEPs are also considered to be PEPs by virtue of business relationships that involve reputational risks similar to those of the relevant PEPs themselves. This is not intended to cover middle ranking or more junior officials in the foregoing categories;
- **STRs** means Suspicious Transactions Reports filed in terms of Section 7 of the Financial Transactions Reporting Act, No 6 of 2006;
- **TF** means the offence of terrorist financing, which was penalized in terms of Section 3 of the Convention on the Suppression of Terrorist Financing Act, No 25 of 2005
- **UNSCR** means the United Nations Security Council Resolutions

Part II

Compliance

Compliance Officer

5. Each Institution is required to appoint a Compliance Officer. The appointed officer should be responsible for the implementation of the Institution's AML/CFT compliance

requirements. The Compliance Officer should have the authority and the resources necessary to discharge his or her responsibilities effectively.

6. According to the management structure of the Institution, the Compliance Officer should report on a regular basis to the board of directors or senior management, or to the owner or chief executive officer of the Institution. The Compliance Officer should be from the senior management level and have direct access to higher management or the board of directors.
7. For consistency and ongoing attention to the AML/CFT requirements, the Compliance Officer may choose to delegate certain duties to other employees of the Institution. For example, the Compliance Officer may delegate an employee in a branch to ensure that compliance procedures are properly implemented at that branch. However, where such a delegation is made, the Compliance Officer remains responsible for the implementation of the AML/CFT compliance requirement.

AML/CFT Compliance Policies and Procedures

8. Each Institution must establish written policies and procedures to assess ML/TF risks. These policies and procedures must be implemented in an effective manner to prevent, detect and remedy instances of non-compliance. It is important that the policies and procedures are communicated, understood and adhered in a timely manner within the Institution. These policies and procedures should be communicated to those who work in the areas relating to customer interactions.
9. Each Institution's AML/CFT compliance policies and procedures must include an assessment of risks related to ML/TF. The assessment must be conducted in a manner that is appropriate to the nature of the Institution's business. This ML/TF risk assessment must be conducted notwithstanding any existing policies and procedures on customer identification, record keeping and reporting requirements.
10. The extent and the level of details of each Institution's AML/CFT compliance policies and procedures will depend on the specific needs and the complexity of the Institution, as well as the Institution's assessed risk to ML/TF.

11. The Institution's AML/CFT compliance policies and procedures must be approved by the senior management and/or board of directors (if any). The AML/CFT compliance policies and procedures must include, at a minimum, ML/TF risk assessment and risk mitigation measures, customer identification and verification, record keeping, submission of mandatory reports to the FIU and ensuring independent audits of the Institution's compliance policies and procedures. For example:
    a) In the case of reporting obligations relating to any suspicion of TF, the compliance policies and procedures of the Institution should include the screening of customers against UNSCR and other lists which are available on the FIU website (http://fiusrilanka.gov.lk) and elsewhere.
    b) Institutions should apply an enhanced level of caution when dealing with transactions involving countries or territories that have not yet established adequate AML/CFT measures that consistent with international standards. Institutions may refer the FATF website (http://fatf-gafi.org) and other sources for this information.

12. Board of directors and senior management are required to understand statutory duties on AML/CFT compliance vested upon the board of directors, the staff and the Institution. Senior management and the board of directors are ultimately responsible for making decisions related to policies, procedures and processes that mitigate and manage the risks of ML/TF within the business.
13. The Institution should have a screening policy when hiring employees to ensure high standards.

Compliance with United Nations Security Council Resolutions

14. The Institution should cross-check whether any customer or beneficiary appears on any designated list issued in compliance with the United Nations Act, No. 45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing (UNSCRs 1267, 1373, 1718, 1540) and any other subsequent Resolutions.

15. It is required to immediately freeze funds, financial assets or economic resources of individuals and entities who are designated by the United Nations Security Council based on such person's/entity's connections with terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing. The Institution should have measures in place to identify and immediately freeze funds, financial assets or economic resources, of such designated persons and entities.
16. Upon freezing or lifting of such freezing of funds, other financial assets and economic resources of designated individuals and entities, or upon the occurrence of an attempted transaction by or for designated individuals or entities, Institutions shall, not later than 24 hours from the time of finding out such customer, inform to the Competent Authority with a copy to the FIU.
17. The Institution should ensure that no funds, financial assets or economic resources are made available to or for the benefit of such designated persons or entities or their beneficiaries.

Risk-Based Approach

18. A risk-based approach is a process that allows the Institution to identify, assess the risks of ML/TF, to develop controls to mitigate the identified ML/TF risks and ongoing monitoring of those controls. Each Institution must use their own judgment, knowledge and expertise to develop an appropriate risk-based approach for their particular organization, structure and business activities.
19. In the context of ML/TF, the risk-based approach is a process that encompasses the following steps:
    A. Identify the ML/TF risk;
    B. Assess the ML/TF risks;
    C. Design and implement controls to manage and mitigate the ML/TF risks;
    D. Monitor and improve the effective operations of the risk based controls.

(A) Identify the ML/TF Risk

20. The Institution must be aware of ML/TF risks inherent to the business activities. As the first step of the risk-based approach, the Institution should identify the ML/TF related risks that may arise from customers, countries or geographical areas and products, services, transactions or delivery channels as well as from proposed innovations thereof. An example of a checklist for their own ML/TF risk identification and assessment is given in Appendix I. By looking at this example, Institutions can prepare a checklist for their own ML/TF risk identification and assessment. This may be not the exact check list for identification of ML/TF risks in every institution. Therefore, Institutions can prepare an own risk identification checklist according to the requirements and the nature of its business.
21. The Institution has to identify the ML/TF risks that may be associated with the products and services that are offered by Institutions due to its vulnerability to ML/TF risks.

(B) Assess the ML/TF Risks

22. A risk assessment is an analysis of potential threats and vulnerabilities of ML/TF to which the institution is exposed. The complexity of the assessment depends on the nature, size and ML/TF risks face by the Institution.
23. When conducting a risk assessment, the Institution has to consider and document the following factors;
    a) Types of customers and business relationships the Institution having with them;
    b) Types of products and services and the delivery channels through which they are offered;
    c) The geographic origins and locations of the customers;
    d) Other relevant factors related to the business activities;
    e) Whether the Customer's name is appearing in UNSCR designated list.

    It is advised to follow the given example for ML and TF risk identification and assessment at the Appendix I. If your answer is "Yes" for any of those items in the example checklist, the Institutions should consider that fact as a high risk for ML/TF.

24. The risk assessment requires detailed knowledge of the business operations and sound judgment exercised by the assessors so the risks for ML/TF can be determined according to each individual factor as well as a combination of factors. The risk assessment will continuously change overtime as the various risk factors evolve.
25. Where the Institution's dealings with a customer are limited to a single transaction (one-off transaction), it is not considered to be an ongoing business relationship. However, the Institution is required to complete a risk assessment of such customer. If the Institution suspects that the transaction is related to an ML/TF offence, then such transactions have to be reported to the FIU as an STR. Please refer part IV for further information.

(C) Design and Implement Controls to Manage and Mitigate the ML/TF Risks

26. Risk mitigation is about implementing controls to address risk factors that are the source of the risk (i.e. threats, vulnerabilities) in a timely manner which is tolerable to the Institution is achieved. Controls should be in the form of written policies and procedures.
27. The Institution may develop and implement the following different types of mitigation measures through the Institution's compliance policies and procedures and internal controls.
    a) Informing senior management about compliance initiatives, identified compliance deficiencies and corrective actions taken;
    b) Ensuring the continuation of the AML/CFT compliance policies and procedures without any disruptions due to changes in management, employees or the structure of the business;
    c) Focusing on complying with mandatory record keeping and reporting requirements including STRs, and adhering to regulations, rules and guidelines issued by the FIU;
    d) Incorporating AML/CFT compliance into job descriptions;
    e) Monitoring employees who handle cash transactions, attend to mandatory reports of AML/CFT measures, suspicious transactions or engage in any other activity that forms part of the AML/CFT policies and procedures;
    f) Increasing awareness of high risk situations within the business;
    g) Increasing the frequency of reviewing ongoing business relationships; and

(D) Monitor and Improve the Effective Operations of the Risk Based Controls

28. The effective management of ML/TF risk is a continuous and dynamic process. The Institution should ensure that the process of managing the risks of ML/TF is subject to regular review and is updated as new or emerging risks are identified, whether caused by changes in the scale or nature of operations, new products, new services, new customer types, etc.

Development of Training and Awareness Programmes

29. The Institution is required to provide training on AML/CFT compliance to board of directors, senior management, employees, agents or any other individuals authorized to act on behalf of the Institution.
30. Such training should consist of raising awareness of the internal policies and procedures for preventing ML/TF. The training programme should provide a clear understanding of Institution's AML/CFT compliance policies and procedures and the related individual's responsibilities.

PART III

Customer Due Diligence

Identification and Verification of Customer and Beneficial Owners

31. Each Institution is required to conduct CDD on customers and beneficial owners, including occasional and one-off customers, when they engage in transactions.
32. If the Institution cannot satisfactorily apply due diligence measures in relation to a customer and/or beneficial owner, the Institution shall not carry out a transaction for that customer. Further, the Institution may also consider submitting an STR to the FIU.
33. If the actions of a customer appear as designed to deliberately avoid CDD requirements, then the Institution should consider submitting an STR to the FIU.
34. Customers and beneficial owners that are identified as high risk should be subject to enhanced due diligence measures such as additional scrutiny and verification of identification information and source of funds.

CDD Measures for Dealers in Precious Metals and Dealers in Precious and Semi-Precious Stones

35. The Dealers in precious metals and dealers in precious and semi-precious stones are required to conduct CDD when the dealer engages in any cash transaction with a customer in Sri Lankan Rupee or in any foreign currency equivalent to or above United States Dollars 15,000.
36. These cash transactions include domestic gemstone/jewellery sale or purchase, gemstones/jewellery imports or exports and, gemstone/jewellery sale or purchase using auctions and exhibitions.
37. CDD in general will be conducted as a minimum requirement. However, when it comes to situations where a customer is identified as of high risk with respect to ML and TF, the Institution should apply enhanced due diligence measures.

CDD Measures for Agents in Real Estate Transactions

38. The real estate agents are required to conduct CDD when they engage in transactions with customers in buying and selling of a real estate property.
39. Real estate agents should be extra cautious about customer/s identity as well as ultimate beneficial owner/s when conducting CDD as there is a possibility of using a front person for buying properties.
40. CDD should be conducted at the time of making an initial deposit or paying an advance for the property.
41. CDD should be conducted for all customers and beneficial owners who will be involved in the same property transaction. Ex. If there is a transfer of the sales agreement or selling that property to another customer or a buyer after making an advance/deposit or any other payment, CDD should be conducted for the new customer/s and beneficial owner/s who appear as new customer/buyer of the property and this should be continued until finalizing the property transaction by registration of the deed.

High Risk Customers/Transactions

42. There are customers / types of transactions / products which may pose higher ML/TF risk to the Institution. In such a situation, the Institution is required to take additional measures. As examples;
    a) Any customer who has links with countries which do not or which insufficiently comply with the recommendations of the FATF (for High Risk and Non-Cooperative Jurisdictions please refer to FATF website (http://fatf-gafi.org);
    b) Any customer linked with a country that has been identified by a national authority as a jurisdiction of concern for drug trafficking, human trafficking, money laundering, terrorism or illicit financing;
    c) any country that has been identified by a reputable organization as having high levels of public corruption;

    (a) Any customer who conducts a complex or unusual transactions, (whether completed or not), unusual patterns of transactions for the customer profile, transactions that match patterns associated with unlawful activity, and transactions which have no apparent lawful purpose;
    d) Domestic and foreign PEPs to include their family members and close associates;
    e) Any customer, transaction or product type that the Institution has identified as posing a higher risk to the business.

Identification of Third Parties

43. The Institution must take reasonable measures to determine whether the Customer is acting on behalf of a third party, where the customer is an agent of the third party who is the beneficiary and/or who is providing the funds for the transaction. In cases where a third party is involved, the Institution must obtain information on the identity of the third party and their relationship with the customer, for CDD purposes.

PART IV

Reporting

Duty of Submitting Suspicious Transactions Reports

44. In making the assessment to submit an STR, the Institution may refer to the list of red flags as mentioned in **Appendix II** – for dealers in precious metals and stones/ **Appendix IV** – dealers in real estate. Industry-specific indicators would also help the Institution to better identify suspicious transactions whether completed or attempted.
45. Each Institution must pay attention to attempted suspicious transactions. If a customer attempts to conduct a transaction, but for whatever reason that transaction is not completed, and if the Institution determines that the attempted transaction is suspicious, the Institution must report it to the FIU.
46. The Institution shall submit STRs using the format as prescribed in Suspicious Transactions (Format) Regulations of 2017, Gazette (Extraordinary) No: 2015/56 dated April 21, 2017 (Schedule V).
47. The Compliance Officer should maintain a register of STRs.

Reporting of Cash and Electronic Transactions

48. Every Institution is required to adhere to the requirements stipulated in Financial Transactions Reporting Regulations No. 1 of 2008, Gazette (Extraordinary) No: 1555/9 dated June 25, 2008.

PART V

Record Keeping

49. The Institution shall take appropriate steps to put in place and maintain a system for record keeping as stipulated in the FTRA, which allows data to be retrieved easily and quickly whenever required, or when requested by the FIU.

PART VI

Penalties for Non-Compliance

50. Failure to comply with the legislative requirements shall lead to penalties. In addition, there may be other actions including regulatory and disciplinary measures against the Institution.

` **Issued on 18 April 2018**

Appendix I

An Example of a Checklist for Institution's ML and TF Risk Assessments

The following checklist is intended to provide an example of how to assess risk for your customers, products, services, delivery channels and geographic locations. This is only a starting point and your institution should customize the checklist according to your business. If you already use another risk assessment tool, you can continue to use it or enhance it as necessary.

If you answer *yes* to any of the questions below, you should consider it as higher risk for money laundering or terrorist financing. Risk-mitigation steps should be taken where appropriate.

	YES	NO	MITIGATION MEASURES
Customer Risk			
Do you have clients that:			
operate in a cash intensive business?			
reside outside Sri Lanka?			
are intermediaries or "gatekeepers" such as professionals that hold accounts for clients where the identity of the underlying client is not disclosed to you?			
are located in a known high crime rate area?			
the nature of their business makes it difficult to identify the true owners or controllers?			
are politically exposed persons?			
do not have an address or who have several addresses without justified reason?			

have a criminal record?			
have links to organized crime?			
Product/Service Risk			
Do you offer products or services that:			
make it difficult to fully identify clients?			
assist in the establishment of a company?			
	YES	**NO**	**N/A**
Do you:			
perform tasks for the purpose of concealing the client's beneficial owner?			
perform tasks of real estate transfer between clients in an unusually short time period without visible legal, economic or other justified reason?			
provide services linked with establishing, operating or managing of a shell company, company in nominal ownership?			
Delivery Channels/Business Relationships Risk			
Do you:			
conduct non-face-to-face transactions?			
Do you have business relationships that:			
involve complicated financial			

transactions?			
involve payments towards/from third persons and cross-border payments?			
involve high risk real estate transactions?			
involve cash payments?			
Geographical Risk			
Do you or your clients operate or undertake activities in the following countries:			
Any country subject to sanctions, embargoes or similar measures issued by the United Nations (UNSCR)?			
Any country identified as a financial secrecy haven or jurisdiction?			
Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement?			
Any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations or as providing funding or support for terrorist activities?			
Any country that is known to have significant levels of corruption, or other criminal activity?			

Appendix II

Anti-Money Laundering/Countering Financing of Terrorism Suspicious Indicators (Red Flags) for Gem and Jewellery Dealers

Customer and customer behavior:

i. Customer executes transaction/transactions which is/are not consistent with his usual profile.

ii. A frequent customer, who buy/sell precious stone/metal or jewellery products makes a transaction/transaction inconsistent with his usual financial status/profile.

iii. Customer does not appear properly concerned about the value, size, quality and/or colour of the precious stone/metal or jewellery product.

iv. Customer pays the value of the precious stone/metal or jewellery producusing an unusual payment method.

v. Customer conducts large or frequent transactions using foreign currency without any economic rationale.

vi. Frequent transactions by a customer especially over a short period of time below the regulatory threshold for customer due diligence, however the total of such transactions is substantial.

vii. Payments received for a purchase of a precious stone/metal or jewellery product from a third party who is not the owner of the funds, without any legitimate business purpose.

viii. Customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping documents.

ix. Customer is unusually concerned and/or makes inquiries aboutthe AML/CFT requirements and internal compliance policies, procedures or controls.

x. Customer attempts to maintain a high degree of secrecy with respect to transactions, for example by requesting not to keep normal business records.

xi. Customer avoids answering questions related to the source of money to buy the precious stone/metal or jewellery product.

xii. Customer is known to have a criminal/terrorism background.

xiii. Customer appears to be related to a country or entity that is associated with ML/TF activities.

Supplier and supplier behaviour:

i. Supplier under/over invoice the value of the precious gemstone/metal.
ii. Supplier uses third parties in transactions related to precious gemstones/metals. Ex: funds paid to a third party who is not related to the supplier without any legitimate business purpose
iii. Precious stones/metals/jewellery products delivered from a third party who is not related to the supplier, without any legitimate business purpose.
iv. Supplier is unable to provide information for due diligence and record keeping purposes
v. Supplier is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes.
vi. The origin of the precious stones/metals/jewellery products appears to be fictitious
vii. Supplier is unusually concerned with the AML/CFT requirements.
viii. Supplier attempts to maintain a high degree of secrecy with respect to the transactions and requests not to keep the normal business records
ix. Supplier is not willing to disclose beneficial owners or controlling interests.
x. For Diamonds:
    a. Rough Diamonds are not accompanied by a valid Kimberley Process (KP) certificate, or broadly recognized equivalent scheme for certification
    b. Ex: No KP certificate attached to the shipment of rough diamonds
    c. The KP Certificate is/appears to be forged
xi. Supplier appears to be related to a country or entity that is associated with ML/TF activities or a person that has been designated as terrorist
xii. Supplier transports precious stones/metal through a country which is associated with ML/TF activities, for no apparent economic reason.

Appendix III

Case Studies as Examples of ML & TF through Dealing in Precious Metals and Precious and Semi Stones:

Case study 1 - Trading gold to legitimize the proceeds of drug trafficking

The police of "country A" investigated that the illicit proceeds gained through drug trafficking has been used to purchase gold from "M Jewellers" by a drug dealer. These gold purchases were being done by a criminal organization and they have been buying gold from various gem and jewellery dealers using the illicit proceeds earned from the sale of drugs. Thereafter the acquired gold has been sold to many other jewellery shops.

The proceeds of the sale of this gold have been transferred to a third party of "country D" that had links to drug trafficking. By transferring these funds the drug dealer laundered his illicit proceeds by completing the money laundering cycle of placement, layering and integration.

Case study 2 - Sale of Gems to another jurisdiction to fund terrorist activities

It was observed that the "company A" operating in country D has been frequently sending representatives to "country M" offering purchases of precious gemstones above the local market prices. As a result, fund transfers have been observed from country D to country M with very large volumes. The purpose of the transaction indicated was purchase of gemstones. The funds were then withdrawn in the "country M" either as cash or cheque withdrawals immediately after the fund transfers. Later it was revealed that persons who withdrawn funds from "country M" had links with a known terrorist group and the funds has been used to fund terrorist activities.

Appendix IV

Anti-Money Laundering/Countering Financing of Terrorism Suspicious Indicators (Red Flags) for Real Estate Agents: (Red flags copied from relevant typologies)

a) Customer procurements/purchases property in the name of a nominee such as an subordinate or a relative (other than a spouse), or in the name of minors or incapacitated persons or other persons who do not have the economic capacity to carry out such purchases.

b) Customer does not want to put their name on any document that would connect them with the property or submit different names on offer letters to purchase, or closing documents and deposit receipts.

c) Customer tries to hide the identity of the beneficial owner or requests that the transaction be structured to hide the identity of the beneficiary.

d) Purchaser is a shell company and a representative of the company who do not like to disclose the identity of the beneficial owner.

e) Address given by customer is unknown, believed to be false, or simply a correspondence address.

f) Customer does not satisfactorily explain the last-minute substitution of the purchasing party's name.

g) Customer pays substantial down payment in cash and balance is funded by an unusual source or offshore bank.

h) Customer purchases property without inspecting it. It realizes that the customer needs to fund for the property and not much worries about the location or any other characteristic of the property.

i) Customer purchases many properties in a short time period, and seems to have few concerns about the location, condition and anticipated repair costs, etc., of each property.

j) Customer is known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided.

k) Transaction does not match the business activity known to be carried out by the customer.

l) Transaction is entered at a value significantly different (much higher or much lower) from the real or market value of the property.

m) Property is sold in a series of successive transactions each time at a higher price between the same parties.

n) Buyer takes on a debt significantly higher than the value of the property.

o) Customer suddenly cancels / aborts transaction and requests refund either back to himself /herself / itself or to a third party.

p) Customer pays for the purchase entirely in cash (to include electronic funds transfers), especially when such a purchase is large or does not match the known profile of the customer, and especially when the purchase funds are transferred from an offshore jurisdiction.

NB: The above list is only indicative and not complete or thorough.

Appendix V

Case study 1: Real Estate Investments with Criminal Proceeds

Real estate transactions can be used by the money launders in every stage of the money laundering process.

Money laundering is a three-stage process of placement, layering and integration. The following case study is relevant to laundering money by placing proceeds of criminal activities in real estate activities.

An individual called X formed two firms in different countries called Firm A and Firm B in country C and D. X's intend was to conceal his involvement in these firms. Therefore, he used a person as front line and a trust to serve as legal representatives to hide his ownership. One of these firms was in real estate operations and the person appointed as the front line led the firm. By arranging a hedging facility (a back-to-back loan) to hedge against currency fluctuations in two countries he used illegally earned, drug proceeds to operate in these real estate investments. Also, he arranged a bank guarantee between two banks in case of a default of the loan. A banking guarantee was provided by a bank based on the pledged deposit of one of his companies as the collateral for the loan facility. The investigations revealed that the funds deposited for the guarantee was generated by X's drug trafficking activities.

Indicators and methods identified in the case:

- Unwillingness to provide information of the borrower and collateral provider was the main doubt for this case.
- The complex nature of loan arrangements and hedging instruments were involved to conceal layering of criminal proceeds.
- Different complex arrangements to conceal the real ownership of the firms.
- An unexpected loan default by the borrower built up the suspicious of real requirement of having a financial facility.

Case study 2: Misuse of a real estate agent to gain introduction to a financial institution, possible link to terrorist financing

A trustee for a trust established in abroad approached a real estate agent to buy a property in country X. The real-estate agent made inquiries with the bank M to ask whether a loan could be granted. The bank rejected the application, as the use of trusts and non-financial professional services appeared to be purposely done to disguise the identity of the beneficial owner or the real owner. Based on this suspicion, the bank M submitted a suspicious transaction report (STR) to the Financial Intelligence Unit.

At the investigations it was found, one of the members of the board of the trust was found to be related to a bank with suspected links to a terrorist organization.

Indicators and methods identified in the scheme:

- Real estate transactions using trusts.
- Demanding for loan/mortgage facilities.
- Trying to use institutional setups such as bank, trust, real-estate agent.

***Appendices I-V include contents from publicly available AML/CFT resources**